DCI/ICS 83-3237
1 November 1983

MEMORANDUM FOR: [redacted] STAT

FROM:

SUBJECT: Computer Security

1. As you know, a computer security (COMPUSEC) project, under the direction of Dr. Ruth Davis, was initiated by the IC Staff this past April. As part of that program, Dr. Davis would like to highlight those aspects of the COMPUSEC program that will require funds so that agency programming guidance for FY 1986 can alert selected agency activities of the potential impact of this program.

2. Request your review, concurrence, and subsequent transmittal of the attached item to [redacted] for his consideration and appropriate STAT action. Additional details will be forthcoming in the DCI's program guidance in January 1984.

[redacted]

cc: [redacted] STAT

Attachment: a/s

STAT

SUBJECT: Computer Security

Distribution (DCI/ICS 83-3237)

Original - Addressee
1 - [redacted] STAT
1 - CIPC Subject
1 - CIPC/Chrono
1 - CIPC/[redacted] STAT
1 - ICS Registry

DCI/ICS/CIPC/[redacted] (1 Nov 83) STAT

DCI/ICS 83-3237/1
1 November 1983

MEMORANDUM FOR: [redacted] STAT

FROM:

SUBJECT: Computer Security

1. As you know, a computer security (COMPUSEC) project, under the direction of Dr. Ruth Davis, was initiated by the IC Staff this past April. As part of that program, Dr. Davis would like to highlight those aspects of the COMPUSEC program that will require funds so that agency programming guidance for FY 1986 can alert selected agency activities of the potential impact of this program.

2. Request your review, concurrence, and subsequent transmittal of the attached item to [redacted] for his consideration and appropriate action. Additional details will be forthcoming in the DCI's program guidance in January 1984. STAT

[redacted]

cc: [redacted] STAT

Attachment: a/s

STAT

SUBJECT: Computer Security

Distribution (DCI/ICS 83-3237)

Original - Addressee
1 - [redacted] STAT
1 - CIPC/Subject
1 - CIPC/Chrono
1 - CIPC/[redacted] STAT
1 - ICS Registry

DCI/ICS/CIPC/[redacted] (1 November 83) STAT

COMPUTER SECURITY

There are major security risks associated with automated handling of compartmented intelligence information. In recent years there has been an explosive trend within the DoD and the Intelligence Community (IC) to automate the processing of sensitive intelligence information. The community today relies heavily on computers, many of which are connected via communication networks, to transmit, process, store and retrieve classified information. The development and use of automated systems have clearly outpaced the parallel development of security programs designed to protect intelligence information. The fact that the theory and practice of computer security has not advanced as quickly as computer utilization and data sharing is of increasing concern to senior policy officials.

Improvement of our present security posture is needed in order to avoid hostile exploitation, unauthorized access and inadvertent compromise. Lack of adequate automated information system security controls causes most computer systems and networks to be vulnerable to the simplest penetration attacks. The threat represented by known and recognized vulnerabilities is of extreme gravity to the Community.

In response to this situation, the leadership of the Intelligence Community, in conjunction with the National Security and Foreign Relations Communities, has a project underway of highest priority to develop an long-term approach to satisfying community computer security requirements. Efforts

to date indicate that the scope of the computer security problem covers six areas of concern; vulnerability and threat, current security measures and processes, Community security roles and responsibilities, technology deficiencies, current policy guidance for security activities, and a DoD/IC action plan.

Immediate steps are being taken to reduce the threat to intelligence information posed by the potentially serious vulnerabilities of computer systems and networks. Systems identified as critical have been nominated as candidates for an evaluation that will assess the system's security and prompt corrective action against shortfalls.

Funds for FY 85 will be requested, where appropriate, to retrofit critical systems with minimum security safeguards. Funds for FY 86 and beyond will be required to support continuing vulnerability assessments and evaluations and to retrofit additional ADP systems with approved safeguards. Moreover funds will be programmed to support and expand the computer security technology base. Each program manager should carefully review the resources being devoted to computer security and provide for increases in funding and manpower levels where appropriate.